⑲日本国特許庁(JP)　⑪特許出願公開

⑫公開特許公報(A)　平2−271466

| ⑤1Int. Cl.⁵ | | 識別記号 | | 庁内整理番号 |
|---|---|---|---|---|
| G 06 F | 15/30 | 340 | | 6798−5B |
| | 15/00 | 330 | G | 7361−5B |
| | 15/30 | 330 | | 6798−5B |
| G 06 K | 17/00 | | S | 6711−5B |

⑬公開　平成2年(1990)11月6日

審査請求　未請求　請求項の数 3　(全8頁)

⑤4発明の名称　データ交換方法及び装置

⑳特　願　平2−8101

㉒出　願　平2(1990)1月17日

優先権主張　㉜1989年1月17日㉝カナダ(CA)㉛588,388

⑦2発明者　マーセル　アルバート　グレイブズ　カナダ国　テイー4アール　3ジエイ7　アルバータ　エドモントン　アベニユー　14008 - 80

⑦1出願人　マーセル　アルバート　グレイブズ　カナダ国　テイー4アール　3ジエイ7　アルバータ　エドモントン　アベニユー　14008 - 80

⑦4代理人　弁理士　吉田　研二　外2名

明　細　書

1．発明の名称

データ交換方法及び装置

2．特許請求の範囲

（1）少なくとも一の携帯型電子装置と、

少なくとも一の端末機と、

前記電子装置と端末機とを結ぶ接続手段と、を含み、

前記携帯型電子装置は端末機が有効であるか否かを確認するための確認手段を有し、

前記端末機は、携帯型電子装置が有効であることを確認する確認手段と、使用者がシステムの使用権を有することを確認する確認手段と、前記携帯型電子装置と端末機との間のインターフェースにおいて伝送されるデータの符号化及び解読を行う暗号化手段と、を有することを特徴とするデータ交換装置。

（2）複数の携帯装置と、

複数の端末機と、

前記各端末機をホストコンピュータに接続する接続リンクと、を含み、

前記携帯型電子装置はデータを保存するためのメモリと、データの処理を行うためのマイクロプロセッサまたは同等の論理ユニット、及びデータ伝送手段を有し、前記メモリ内には使用者を確認するためのデータ及び前記携帯型電子装置が端末機を有効であると確認すると共にデータの交換を実行しあるいはもし端末機が無効である場合にメモリ内のデータを消去させるプログラムを内蔵し、

前記各端末機はマイクロプロセッサまたは同等の論理ユニットと、データを保存するためのメモリと、カードが有効であることを確認するためのプログラムと、走査装置と、使用者と通信するための入出力装置と、必要時に前記携帯型電子装置に電力を供給すると共に該携帯型電子装置と前記端末機との間でデータを伝送するための電力を供給するために携帯型電子装置に接続される電源と、を備えたことを特徴とするデータ交換装置。

（3）端末機が携帯型電子装置を有効であるか否か確認する工程と、

携帯装置が端末機が有効であることを確認する工程と、

前記端末機が使用者の肉体的特徴を走査することによりそのデータを得ると共に、このデータを使用者の携帯型電子装置内に登録されているデータと比較する工程と、

不正なアクセスが行われる得る場所であるインターフェースで暗号化手段を用いてデータの符号化及び解読を行う工程と、

無効な端末機にて通信が試みられた場合に携帯型電子装置のプログラム及びデータを消去する工程と、

携帯型電子装置が無効である場合、または有効であっても正当な使用者でない場合に端末機によって携帯型電子装置の受入れを停止するか拒否する工程と、

電力供給が中断したときに端末機内のデータ及びプログラムを消去させる工程と、

電力供給が停止した後、正当な使用者が携帯型アクセス装置を用いて端末機の電力を回復させる工程と、からなることを特徴とするデータ交換方法。

3．発明の詳細な説明

〔産業上の利用分野〕

本発明は顧客の持つカードなどの携帯型電子装置を端末機に適用することによって不特定多数の利用に供される、例えば自動クレジット及び再取引き、パスポート及び旅行ビザの認証、健康及び医療関係の登録、証券取引及び各種許可証の付与などに使用される装置における不正行為の対応手段に関する。

〔従来の技術〕

磁気帯などを用いて若干の記憶機能を備えたカード等の携帯装置及びこの携帯装置が接続される端末機を用いたデータ交換システムが周知であり、通常該システムの各装置は所定の地域におけるサービスへのアクセスを制御するために使用されることが多い。

一般には、端末機はＣＰＵまたはコンピュータに接続され、これらが前記アクセス作用を制御すると共に端末機に挿入されるカード上のデータの最終記憶保存手段としての機能も果たしている。

英国特許第１５０４１９６号（モレノ）にはこのようなデータ交換システムの一例が開示され、携帯装置及び中央コンピュータに接続された周辺装置あるいは端末機が含まれている。該モレノ特許明細書において言及されている携帯装置の大部分は磁気トラックメモリを使用しているが、このメモリには極めて容易に不正な加工を加えることができ、またその記憶内容が読み出されてしまうという欠点がある。

加えて、その記憶容量も極めて小さく、さらにはメモリ自体が例えば不注意で磁性体の近傍に放置されるなどのアクシデントによってその記憶データの乱れが容易に生じてしまう。

この結果、このようなメモリを用いた装置は詐欺など不正行為の格好の的とされていた。

一方、米国特許第３７０２４６４号にはこのような低記憶容量と記憶データの揮発性という問題を解決するため、ＩＣメモリを組み込んだカードを携帯装置として使用する構成が開示されている。

しかしながら、このような装置によってもメモリの内容が読み出されたり抽出あるいは変更が加えられることを阻止することはできない。

前記モレノ特許は携帯装置のメモリにおける禁止領域からのデータの読出しあるいは書込み作用を防止するための禁止手段を付加することによってこのような不都合の解決を図っている。

この手法を用いる場合、携帯装置自体が固有の禁止手段を内蔵していることが上述の不正詐欺行為を阻止する上で重要な条件となるが、モレノ特許においてはこの禁止手段は周辺装置内に組み込まれているため、携帯装置であるカード内に記憶されているデータへの干渉には全く効果を発揮することができなかった。

英国特許第１５０５７１５号にはこの種のデータ交換システムの開示が見られるが、周辺装置にエラーが発生した場合にこれが直接中央コンピュータに告知される構成は取られておらず、周辺装置には携帯装置から得られたデータを周辺装置に

伝送するための書込み機構が内蔵されており、該周辺装置においてデータが第２の携帯装置に書き込まれるという構成が取られている。この第２の携帯装置はその後所定の基準ベースに集められると共に中央コンピュータによりそのデータが該中央コンピュータのメモリへ転送記憶されることになる。

他方、カナダ国特許第１２０７４６号には認可された団体から提供されるサービスへのアクセスを許可する方法及び装置が提案されている。

このシステムはメモリ及びマイクロプロセッサを内蔵した携帯カードを含み、システム側ではこのカードと通信すると共に所定のコンピュータプログラムを実行させる事が可能に構成されている。

前記カードとシステムとは互いに等しい実行アルゴリズム及びこのアルゴリズムが動作したときに適正なアクセスを許可するよう機能する秘密データを備えている。

ところが、このようなシステムには相当に複雑な構成が要求されると共に団体側に操作者を置く必要があり、人件費がかさむ。

さらには、使用者を確認するために携帯カード上に予め登録されている指紋を符号化するという技術も周知である。英国特許第２１８５９３７Ａ号には登録された使用者の指紋をコンピュータ処理した画像を記憶したクレジットまたは同種のカードが開示されている。そして、データ処理を許可するか否かは指紋読取り器により使用者の指紋を走査してその結果をカード上の記録データと比較参照する。両方の指紋が合致したときにシステムへのアクセス許可が使用者に出るということになる。このような装置は現在既に商業的に採用されている。

［発明が解決しようとする課題］

しかしながら、このような上記各システムは全て詐欺的行為、不正なアクセス及びカードまたは端末機内のデータの偽造などに晒され易く、またその構成が非常に複雑化してしまうという欠点が否めなかった。

発明の目的

本発明は上記従来の課題に鑑みなされたものであり、その目的は団体が提供するサービスへのアクセスに関して高度な安全性と詐欺的不正行為防止機能を備えたデータ交換装置及び方法を提供することにある。

［課題を解決するための手段及び作用］

本発明は、カード端末機によるサービスのアクセスを許可するシステム及び方法に対し、高度な詐欺防止効果を発揮する。

本システムはカード等からなる携帯装置、端末機などからなる周辺装置、そして本システムの特徴的機能には必ずしも必要ではないが大規模のシステムに適用する場合に選択的に用いられる遠隔走査によるホストコンピュータを含む。

これらの各構成要素は電気コネクタ、光ファイバーあるいは無線伝送など所定の通信媒体にて互いに接続されている。

前記端末機はマイクロプロセッサまたは同等の論理装置及びメモリ、カード読取り装置及び指紋走査器を含む。

本発明において特徴的なことは、前記カード（携帯装置）がマイクロプロセッサまたは同等の論理装置及びメモリを内蔵してカード側から端末機に対して端末機が有効であるか否かを能動的に確認する機能を備え、端末機が正当な適合するものであると判定されない限り、カードがデータ読出しを許可しない構成としたことにある。

前記カードは、電子的にまたは光学的あるいは無線伝送など任意の手段を用いて端末機に接続される。

前記カードと端末機とは互いに固有のデータ及びプログラムが組み込まれている。

従って、カードがリーダに挿入されるとマイクロプロセッサまたは論理ユニット及びメモリ内のプログラム及びデータによってまず確認作用が実施される。

前述したように、前記カードは端末機が有効であるか否かを確認し、逆に端末機はカードが有効であるか否かそして指紋走査器によってカード内に予め記憶登録されている指紋データと使用者の

指紋等を比較参照して本人であるか否かを確認する。

勿論、本システムにおいてはこのような指紋照合に限ることなく他の肉体的特徴例えば目の網膜またはＤＮＡ走査を利用する場合にも勿論適用可能である。

また、システムの各構成装置間でデータが行交う場所には符号化及び解読機能作用を行わせることによってよりシステムの安全性を一層向上させることもできる。

本発明は少なくとも一の携帯型電子装置と、少なくとも一の端末機と、前記携帯装置と端末機とを接続する通信手段と、を含み、前記携帯装置は端末機が有効であるか否かを確認するための確認手段を有し、他方前記端末機は携帯装置が有効であるか否かを確認する確認手段及び使用者がシステムの使用許可を得ているものであるか否かを確認するための確認手段とを含む。

さらに、端末機への干渉を防止するための保護手段及び携帯装置と端末機との間におけるインターフェースでのデータの符号化及び解読を行う暗号化手段を供えている。

また、本発明に係る複数の携帯装置、複数の端末機及び各端末機をホストコンピュータに接続する接続リンクを含むシステムへの不正なアクセスを防止するための方法においては、前記携帯装置には該携帯手段自体及び及び使用者の確認媒体となるデータが内蔵され、端末機が携帯装置に接続されてこの携帯装置に電力が供給されると端末機は携帯装置が有効であるか否かを判定し、有効でない場合にはこの携帯装置を拘留するかその受け入れを拒否する。他方、逆に携帯装置側も端末機が有効な端末機であるか否かを判定し、有効でない場合には該携帯装置はそのメモリ内のデータを消去して端末機に悪影響を及ぼすことを回避する。

そして、端末機はその後使用者の肉体的特徴を走査すると共にそれによって得られたデータを携帯装置内に予め記憶保存されているデータと照合して使用者が携帯装置と端末の使用許可を有するものであるか否かを判定する。

もし携帯装置と端末機とが有効であり使用者に使用権があるならばサービスが開始され、他方そうでない場合にはカードが拘留されるかあるいは受入れが拒絶される。

端末機への電力供給が停止し端末機のプログラムとデータとが消去されると、その後は使用権を有する者がそのアクセス携帯装置を適用した場合かあるいはホストコンピュータからの指令が出た場合にのみ再装荷可能となる。また、携帯装置と端末機との間のインターフェース及び端末機とホストコンピュータとの間のインターフェースには暗号化手法が採用される。

［実施例］

以下、図面に基づき本発明の好適な実施例について説明する。

知能カードは、知能端末機、指紋読取り装置及びカード使用者及びカード発行者に対し可能な限り最大の保護を確保するためにホストコンピュータとインターフェースを介して接続するよう組合せることが最も望ましい。

第１図及び第３図は本発明に係る装置の外観及びその基本的なハードウェアの構成をそれぞれ示す。

ホストコンピュータシステム１にはパーソナルコンピュータ、ミニコンピュータ、メインフレームあるいは特定の用途に使用される任意のコンピュータ装置を使用可能である。

このホストコンピュータシステム１はモデムを介して電話線などの適当な接続手段２にて端末機３に接続されている。勿論、電話線に限られることなく他の接続手段例えば無線通信、ダイレクトケーブルまたは光ファイバなども使用可能である。

端末機３は図示例においては知能端末として構成され、ディスプレイ５または音声合成器あるいは他の使用者との交信用手段、そしてカード４に対するデータの読取り及び書込みを行うためのカードリーダ６が含まれている。

また、この端末機３には該端末にデータ入力するためキーボードあるいは他の手段からなる入力装置８及び使用者の肉体的なデータを得るための

指紋走査器７または他の装置を備えている。

以上のような構成の下に、使用者が端末機３のサービスを受けるためにカード４を用いたアクセスを得る際、システムはまず特定の個人であることを確認するための手続きを要求する。

使用者がカード４を端末機３に挿入すると、該端末機３自身がこのカード４によって確認される。そして逆に、このカード４は端末機３により確認されると共に該カード４の発行時にデジタル方式で登録された使用者の指紋がこの使用時に指紋走査器７により読み取られた使用者の指紋と照合される。勿論、この本人確認ステップにおいては、他の例えば暗証番号なども併用することが可能である。

もし、カード４の挿入された端末機３が適合しないものであることが判明した場合にはこのカード４は端末機３内のメモリの記憶データを消去してその後に使用する他人によってデータが悪用されることを阻止する。

不適合なカードであることが判明した場合にはこのカードは端末機３に拘留されるかあるいは正当な使用者により回収される。

また、指紋照合の結果指紋が合致しないことが判明した時にはカードが拘留され、そうでない場合には使用は許可されて端末によるサービスが開始することになる。

第２図に以上のように構成される本願発明に係る装置の動作フローチャートを示す。

実施例において、カード４はそれ自身のマイクロプロセッサまたは論理ユニット、メモリ及び、そしてデータ及びプログラムを内蔵するいわゆる知能カードからなる。

そして、このカード４自体は独立した電源は持たないが、端末機３へ挿入された時に該端末機３から電力供給を受けるように接続がなされる構成となっている。

勿論、カード４自身が固有の電源を持つ構成とすることも好適である。

以下、第２図を参照しつつ本発明の動作について説明する。

装置動作は、カード４を端末機３のカードリーダ６に挿入することで開始する（２００）。

まず、本人の確認工程に入る。端末機側がカード４に対して電力を供給する（２０１）と共に、所定の質問信号を発生する（２０２）。カード４側では、電力供給（２０３）及び質問入力（２０４）を受けると、この端末機３からの質問に対し所定時間内でチェックを受けることになる（２０５）。この時、もし質問が到達しない場合にはカード４はそのメモリ内に保存されている全てのデータを無効とし、これによって使用不可能になる（２０６）。

端末機３が質問を行っていることが確認されると、カード４からこの質問に対する回答が行われる（２０７）。

端末機３は、カード４からの回答が所定時間内に返ってきたか否かを判定し（２０８）、Ｎｏである場合にはカードを拘留するかその受け入れを拒否する（２０９）。

時間内に回答があったならば、その回答が正しい（所定の内容である）か否かが判定される（２１０）。

このようにして、カード４と端末機３とが共に適合するものであることが判明すると、入力された指紋の処理が端末機３側とカード４側とで平行して進行することになる。

なお、本願発明は以下のような異なった種類のカードのいずれにも適用可能である。

（１）パスポートカード
（２）クレジットカード
（３）証券取引きカード
（４）許可証カード
（５）負債カード

従って、このようなカードの種類に従って当初の質問に対する回答も異なることになる。この識別は端末機３が当該対象となっているカードを判別することにより行われる。

ステップ２１０における判定結果がＮＯである場合には、カードの拘留または受入れの拒絶がなされる（２０９）。

次に、使用者と当該カードの所有者との確認工程に入る。これは、指紋照合により行われる。

まず、使用者の指紋を走査する（２１１）。

ここで、カード４側ではこの指紋データ照合工程に入る前にカード４内のメモリから指紋データを読み取れるか否かを確認し（２１２）、Ｎｏである場合には該カード４は端末機３内の使用者の走査された指紋データを消去する（２０６）。

ステップ２１２において指紋照合を実行可能であることが判明すれば、カード４はその内部に予め登録されている指紋データを端末機３へ供給し（２１３）、端末機３はこれを受けて（２１４）使用者が本人であるかどうかを判定する（２１５）。

そして、ステップ２１５の結果がＹｅｓである場合、即ち使用者が当該カード４の真正な使用権を有する者であることが確認されると、ここで初めてカードメモリへのアクセス許可（２１６）及びシステムへのアクセス許可（２１７）が出され、Ｎｏである場合にはカードの受け入れ拒否又は拘留（２０９）が行われることとなる。

尚、以上の確認工程の所要時間は必ずしも厳密に定められているわけではないが、約２５秒前後以上掛ることほぼないといって良い。

また、第三者が端末機３を工作してその内部のデータまたはソフトウェアに不正に手を加えるというような事態が生じる可能性もある。

これを防止するため、端末機３内における全てのソフトウェアはＲＡＭ上にのみ書き込まれている。従って、不正工作により端末機３への電力供給がこの工作時に停止したならば直ちにそのＲＡＭ内のデータが揮発し、悪用されることを有効に回避することができる。

そして、特別のアクセス用携帯装置を持つ許可を受けている技術者だけがその携帯装置またはホストコンピュータから新しいソフトウェアを端末機３へ落すことができ、この端末機３を再び使用可能状態に置くことができる。

第３図に係るブロック図は単一の端末機３のみを含む１システムの好適な構成例を示すものである。

ホストコンピュータシステム１は端末機３から遠く離れた位置に配設されており、両者は電話線２及びモデム１０ａ及び１０ｂにより互いに接続されている。

端末機３はＰＣ型母盤９を含み、この母盤９はマイクロプロセッサまたは他の論理装置及びメモリ、知能カードリーダ６、指紋走査器７、カスタムキーボード８及びディスプレイ５を有する。

カードリーダ６は知能カード４を受け取ると共にデータの交換を行う。

知能カード４はほとんどの場合マイクロプロセッサまたは他の論理装置及びメモリを内蔵している。

そして、このような処理に対応したソフトウェア及びデータは端末機３及び知能カード４内に記憶保存されており、これらによって第２図のフローチャートに示した確認処理工程が実行されることになる。

知能カード４はマイクロプロセッサまたはいくつかの論理ユニット及びメモリチップを内蔵したプラスチックまたは他の媒体を用いた特殊技術により製造されるものである。従って、このカード４は自己の記憶及び処理双方の機能を備えている。実際上、このようなカードはポケットサイズのコンピュータシステムを構成しており、その適用可能範囲は非常に広い。

本システムには多種類の入手可能な素子を利用することができる。

例えば、端末機３の母機にはＩＢＭ　ＰＣ（商品名）、カードリーダ６としてＴｏｓｈｉｂａ　ＦＺ１３１８（商品名）、指紋走査器７としてＩＤＥＮＴＩＸ　Ｔｏｕｃｈｓａｖｅ　Ｔ５－５００（商品名）などを使用可能である。

また、知能カード４としてはＴｏｓｈｉｂａ　ＴＯＳＭＡＲＴ　ＣＺ－３０００（商品名）が好適である前記ＩＢＭ　ＰＣは多くの場合ホストコンピュータ１１として用いられるが、多数の端末機３を有する大規模で複雑なシステムを使用する場合には、例えばメインフレームなどの大型コン

ピュータが必要となる。

また、図示例では、電話線とモデムを接続機器として用いているが、他の連結手段、例えばビルディングの保安システムなどによれば、モデムを用いることなくホストコンピュータや複数の端末機を接続することの可能な専用通信ケーブルを利用できる。

更に、無線あるいは光学的な接続手段を使用しても良い。

最後に、以上のシステムにおいて一層安全性を向上させるため、ホストコンピュータと端末機との間でデータ伝送を行う前にデータを符号化し、受信後にこのデータを解読するという暗号化技術を採用することも好適である。勿論、この符号化及び解読技術は知能カードからデータの読取り及び書込みを行う場合にも同様に適用され得る。

本発明は上記構成に限ることなく、その開示範囲内で任意にその構成を変更して異なる形態として応用することも勿論可能である。

［付記］

（1）請求項（1）に記載の装置において、前記携帯装置はマイクロプロセッサまたは同等の論理装置、メモリ、データ伝送手段及びカードと端末機との間の通信を実行するインターフェースを内蔵していることを特徴とするデータ交換装置。

（2）上記（1）に記載の装置において、前記端末機は、入力手段、出力手段、使用者の肉体的特徴を走査するための走査装置、カードリーダ、マイクロプロセッサまたは他の論理ユニット、メモリ及びデータ伝送手段を含むことを特徴とするデータ交換装置。

（3）上記（2）に記載の装置において、前記入力手段はキーボードからなり、前記出力手段はディスプレイからなることを特徴とするデータ交換装置。

（4）上記（3）に記載の装置において、前記通信手段は電話線と一または複数のモデムを含むことを特徴とするデータ交換装置。

（5）上記（4）に記載の装置において、前記確認手段はコンピュータプログラムまたはプログラムを含むことを特徴とするデータ交換装置。

（6）上記（5）に記載の装置において、前記確認手段はさらに指紋走査器及び走査して得られた使用者の指紋データを携帯型電子装置内に予め記録保存されている指紋データと照合するコンピュータプログラムまたはプログラムを含むことを特徴とするデータ交換装置。

（7）上記（6）に記載の装置において、前記保護手段は電力供給が途絶えた時にその内蔵データを失う揮発性メモリを含むことを特徴とするデータ交換装置。

（8）上記（7）に記載の装置において、前記端末機内のマイクロプロセッサ及びメモリはＩＢＭの母機であることを特徴とするデータ交換装置。

（9）請求項（1）に記載の装置において、前記端末機はさらに通信手段及び暗号化手段を介してホストコンピュータに接続されていることを特徴とするデータ交換装置。

（10）上記（9）に記載の装置において、前記通信手段は1または複数の電話回線及びモデム、ダイレクトケーブル、そして無線及び光学的伝送手段を含み、また暗号化手段は端末機とホストコンピュータとの間のインターフェースにおいてデータの符号化及び解読を行うために使用されることを特徴とするデータ交換装置。

（11）請求項（2）に記載の装置において、前記携帯装置には専用の独立電源を備えていることを特徴とするデータ交換装置。

（12）請求項（2）に記載の装置において、前記ホストコンピュータはＩＢＭ　ＰＣであることを特徴とするデータ交換装置。

［発明の効果］

以上説明したように本発明によれば、携帯装置側に端末機を能動的に確認する機能を持たせると共に、端末機内における全てのプログラム及びデータは揮発性のメモリ内に記憶させて、外部からの工作などで手が加えられて電力供給が停止すると同時にそのデータが全て失われるように構成したので、不正な使用によって装置の安定性が侵やかされるという不都合は完全に阻止され、第三者

による本人以外のデータの悪用が生じることはない。

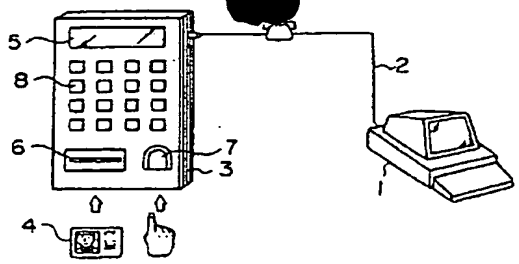
4．図面の簡単な説明

第１図は本発明装置の外観斜視図、

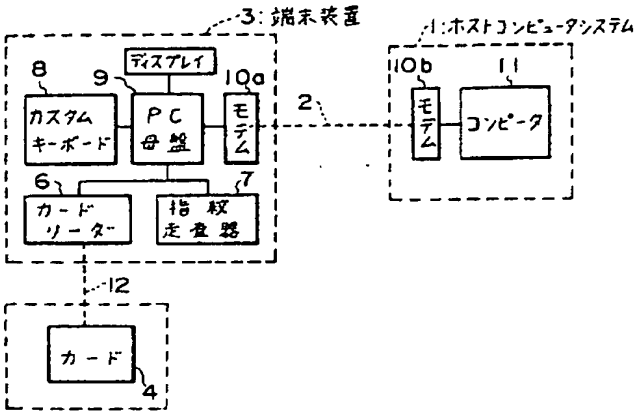
第２図は本発明方法の動作のフローチャート図、

第３図は本発明装置の内部構成ブロック図である。

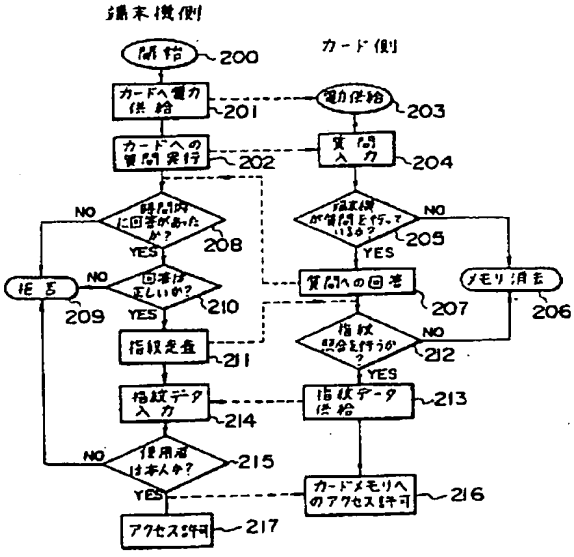
１　…　ホストコンピュータ装置
２　…　接続ライン
３　…　端末機
４　…　カード
５　…　ディスプレイ
６　…　カードリーダ
７　…　指紋走査器
８　…　キーボード
９　…　ＰＣ母盤
１０　…　モデム
１１　…　コンピュータ




第　１　図




第　３　図




第　２　図